U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 2, 2007

The Honorable Edward Markey
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Markey:

It is my pleasure to provide the following responses to your committee's May 10, 2007 request, concerning the Transportation Security Administration's (TSA) information security policies and practices.

Theft of TSA Hard Drive

1) **Was the information contained on the TSA laptop that is presumed stolen protected using encryption or alternative methodologies or technologies that render data in electronic form unreadable or indecipherable by unauthorized users? If not, why not?**

   The external hard drive was not protected with encryption or other electronic security technology. TSA's Office of Inspection is conducting a criminal investigation with the assistance of the Secret Service and the Federal Bureau of Investigation, and is also conducting an administrative review of this incident. However, all TSA employees are trained to identify and protect sensitive data of any type to include Personally Identifiable Information (PII) and Sensitive Security Information (SSI) through required Online Learning Courses and policies established by TSA's Chief Information Officer (CIO) and Privacy Office.

2) **What specific personnel information did the missing hard drive contain?**

   The external hard drive contained historical payroll transaction data including name, social security number, date of birth, address, time and leave data, financial allotments and deductions, bank account and routing information, and other payroll and accounting related data.

3) **How long does TSA maintain personal information belonging to former TSA employees?**

   The National Archives and Records Administration (NARA) approved TSA's records disposition schedule for the Office of Human Capital (OHC) on August 31, 2004 (Job No. N1-560-03-8). The OHC schedule met NARA's basic standards and has been implemented TSA-wide via the Records Management Files Classification System. The disposition for Personnel records is consistent with the General Records Schedule (GRS) 1, *Civilian Personnel Records*. The disposition for Payroll records is consistent with GRS 2, *Payrolling and Pay Administrative Records*.

TSA retains records from the Official Personnel Folder (OPF) of former employees in accordance with GRS 1 *Civilian Personnel Records*. Specifically, separated employees' permanent records in their Official Personnel Folders are retained for 30 days after separation. The records are then sent to the National Personnel Records Center (NPRC) where they are destroyed 65 years after separation.

Employee payroll records are kept in accordance with GRS 2 *Payrolling and Pay Administrative Records*. Individual employee pay records containing pay data on each employee within the agency are kept in accordance with GRS 2(1) and are transferred to the National Personnel Records Center (NPRC) and destroyed when 56 years old.

A complete listing of all of the retention periods for personnel and payroll records relating to current and former TSA employees can be found in the agency's NARA approved file plan 1100 Human Resources **(ENCLOSURE 1).**

4) **Does TSA have a data retention policy for handling the personal information of its former employees? If not, why not? If it does, please provide the Committee with a copy of this policy.**

TSA's Records Management System provides the policies and procedural guidance for all records TSA generates and manages. Annual mandatory training is also provided to all TSA employees and contractors on their responsibilities for the handling of all TSA records. On the TSA intranet website, accessible to all TSA employees and contractors, TSA has published Records Management guidance and TSA Management Directives (MD) for the creation, maintenance, and proper disposition and handling of TSA records. These include mandatory instructions, as listed above, for handling OHC records on current and former employees. The guidance and MDs include:

- TSA MD 200.7, Records Management (Assistant Administrator for Finance and Administration and Chief Financial Officer, October 9, 2002), provides policy for the TSA Records Management program **(ENCLOSURE 2)**;

- TSA MD 200.8, Records Management Files Classification System (Assistant Administrator for Finance and Administration and Chief Financial Officer, January 28, 2005), establishes TSA policies and procedures for a unified Records Management Files Classification System for organizing and identifying files or documents to speed the retrieval, use and disposition of TSA records **(ENCLOSURE 3)**;

- TSA Records Management Guidance (Assistant Administrator for Finance and Administration and Chief Financial Officer, November 15, 2002), provides general guidance on creating and maintaining TSA Records **(ENCLOSURE 4)**; and,

- TSA Records Management Policy Manual (Assistant Administrator for Finance and Administration and Chief Financial Officer, December 20, 2002), defines the mission and principles of TSA's Records Management program, incorporates applicable Federal requirements into standard practices, identifies basic Records Management program

requirements, and sets forth responsibilities for TSA Records Management **(ENCLOSURE 5)**.

Security Weaknesses on TSA's Watchlist Redress Web Site

1) **From October 6, 2006 through February 14, 2007, the TSA watchlist redress website contained an insecure link. During that time, an estimated 200 users accessed the system through this link. Did the individuals whose information may have been compromised during that time period receive notification from TSA alerting them of the potential risk to their personal information? If yes, describe the method of notification.**

   All individuals who accessed the site via an unsecured link were sent a letter from TSA stating:
   - one of the links was not encrypted as it should have been;
   - the risk of compromise is extremely low;
   - there are a few precautionary steps that they may want to take;
   - TSA will not contact the individual to confirm any personally identifiable information; and
   - TSA apologizes for any inconvenience that this action may have caused.

2) **Please provide the exact number of individuals that accessed the site during the time period in (1) above.**

   Two hundred forty-seven individuals accessed the unencrypted link on the TSA Redress website. An additional link located on the same page was encrypted. Information provided to TSA via that link was secure.

3) **Please provide the number of individuals that received notification and the number of people whom TSA was unable to notify, if any. For those individuals for whom notification was not effective, please describe any and all additional means of notification employed by TSA.**

   TSA sent letters to the 247 individuals who accessed the redress website using the unencrypted link. Of these, four individuals either did not provide complete addresses and/or telephone numbers or provided invalid addresses and/or telephone numbers in their redress request. Therefore, TSA's attempts to reach these four individuals were unsuccessful.

4) **If the method of notification was in writing, please provide a copy of the notification letter.**

   The method of notification was in writing and also posted to the DHS web page **(ENCLOSURE 6)**.

5) **Please provide a listing of remedies (e.g., credit monitoring service) that TSA is offering to individuals who clicked on the insecure link.**

   TSA is providing individuals with a benefit package to provide employees and former employees affected by the data security incident with free credit monitoring for up to one year. Credit monitoring services will include monitoring of all three national credit bureau reports, fraud alerts, detection of fraudulent activity and identify theft, and fraud resolution and assistance. In

addition to the credit monitoring, the package includes ID theft insurance up to $25,000, fraud alerts and identify restoration specialists who will complete paperwork and assist employees in the event they are a victim of identity theft.

In addition, TSA sent letters to affected individuals and provided a list of precautionary steps that these individuals could take to protect themselves from possible identity theft to include:

- TSA advised individuals to call any one of the three credit reporting agencies and provided the phone numbers listed below. TSA specifically advised individuals to: 1) request that a fraud alert be put on their account, and 2) order a free credit report from the agency. TSA recommended that individuals request a free credit report from each agency with a four month interval between requests (i.e., a request to one agency, allow four months, and then submit a request to the next agency). By spacing the requests, individuals can monitor their credit over time.

    - Equifax 1-800-525-6285
    - Experian 1-888-397-3742
    - Trans Union 1-800-680-7289

- Review their credit reports carefully when they receive them for accounts they did not open or for inquiries from creditors that they did not initiate. TSA also advised them to review their personal information for accuracy and to call the credit agency at the telephone number on the report if they find anything that does not appear to be accurate.

- File a report with their local police department if they find any suspicious activity on their credit reports.

- Obtain additional information about identity theft from the Federal Trade Commission's website: www.consumer.gov/idtheft.

Shortly after discovery of the non-secure link, TSA shut down the site and TSA's Office of Inspections initiated an inquiry into the matter. This inquiry is currently ongoing.

6) **Does the Department utilize a policy that prescribes the frequency of audits for its Web sites to ensure their security and accuracy? If yes, please provide a copy of this policy.**

DHS policy (Sensitive System Handbook 4300A, V.5.1 - April 18, 2007) requires that annual system security assessments and continuous monitoring be conducted in accordance with National Institute of Standards and Technology (NIST) Special Publication SP 800-53, "Recommended Security Controls for Federal Information Systems" **(ENCLOSURE 7)**. In accordance with the NIST 800-53 methodology, both human monitoring and automated vulnerability scan tools are used by DHS to monitor the security of information systems. Security controls are tested with a frequency depending on risk, but no less than annually, as specified by SP 800-53.

EXCERPT FROM 4300.A **(ENCLOSURE 7)**:

3.9.11 "Annual Self-Assessments

NIST SP 800-26, Security Self-Assessment Guide for IT Systems, provides the IT security requirements that the DHS IT Security Program must satisfy for the FISMA annual review requirements. NIST SP 800-26 directs the use of an extensive questionnaire to determine whether the objectives of security controls installed in unclassified systems are being met. These guidelines are most often employed for identifying weaknesses or areas of needed improvement.

For FY 2007 and beyond, FIPS 200/NIST SP 800-53 must be used for the specification of security controls, and NIST SP 800-53A must be used for the assessment of security control effectiveness and for the annual FISMA reporting.

The annual assessments are performed within the Continuous Monitoring Phase of the accreditation, the purpose of which is to provide ongoing oversight and monitoring of the security controls in the IT system and to inform the authorizing official or designated representative when changes occur that may impact the security of the system. During this phase, the status of the IT system is monitored to ensure that residual risk is kept within an acceptable level, and any significant changes to the system configuration or to the operational/threat environment that might affect system security are identified. DHS Components must re-accredit their IT systems every 3 years or whenever a major change occurs, whichever occurs first."

7) **Was such a policy utilized prior to the detection of the security weakness at TSA's watchlist redress site?**

The TSA Redress site was hosted by Desyne.com. Absent specific contract language, the penetration testing team is not allowed to perform tests on systems hosted outside of TSA due to potential liability concerns. After thorough review, the TSA Redress system was scheduled for penetration testing before the end of Fiscal Year 2007.

8) **How often are the Department's Web sites monitored for security and accuracy, and how is such monitoring performed? Please indicate whether this monitoring is achieved through automated tools solely or whether the process also includes human monitoring.**

For clarity, please see response 6 for DHS policy **(ENCLOSURE 7)**.

9) **We understand that the development of the site was performed by a contractor, Desyne Web Services, Inc. Does TSA continue to contract the services of Desyne Web Services, Inc. for this website or any other TSA website?**

Yes, TSA contracts with Desyne for the maintenance and support of the DHS Traveler Redress Inquiry Program (DHS TRIP), Claims Management System (CMS), and School Bus Transportation Security Awareness (STSA) Training Application web applications. The TSA-sponsored Traveler Identity Verification Program website is no longer in operation since DHS TRIP was launched in February 2007.

10) **If the contract with Desyne is no longer in effect, please indicate when the contract became inactive and whether the conclusion of the contract was prompted by TSA. If the contract was concluded by TSA prior to the expiration of the term, please indicate the rationale for the termination.**

The period of performance of the aforementioned contracts has not ended and TSA has not terminated the contracts.

11) Does the Department or any of its components utilize the services of Desyne Web Services? If yes, please provide the contract number and dollar value of those contracts.

The only DHS entity that has an active contract with Desyne Web Services is TSA. The following are the active contracts with TSA that utilize the services of Desyne Web Services:

Contract	Contract Number	Value	Expiration
BACKUP SYSTEM	HST01-06-C-FIN110	$98,000.00	09/30/2007
CMS Maintenance	HST901-06-C-FIN111	$71,212.50	08/30/2007
CMS Server Hosting	HSTS03-04-P-AOT134	$81,386.00	08/31/2007
DHS Traveler Redress Inquiry Program TRIP[1] (formerly TSA's Redress Program)	HSTS03-P-OSC001	$269,611.00	04/20/2008

Note: STSA contracted with Consolidated Safety Sources (CSS), contract number HSTS002-05-C-MLS508, to design, deliver, and host the School Bus Security Training. CSS subcontracted to Willetts Systems Incorporated. Willetts Systems Incorporated subcontracted with Desyne Web Services for hosting.

12) TSA, through its online watchlist redress site, is collecting personally-identifiable information on a significant number of individuals. What data safeguards are in place to ensure that this information is secure? Is this information encrypted in transit and in storage? Is this information retained after an individual's case has been resolved? If yes, why, how long is the retention period and how is this information ultimately disposed of?

Personally-identifiable information transmitted to TSA through its online Watchlist redress site was encrypted in transit. It was not encrypted in storage. TSA's redress site is no longer in operation instead TSA is operating DHS TRIP.

TSA has a records retention schedule that is pending approval at the National Archives and Record Administration (NARA). In the schedule, TSA proposes retaining case records as follows:

- TSA's Records for Misidentified Individuals are kept by TSA for seven years after issuance of a final agency decision. After the issuance of the final agency decision, records would be transferred to NARA and may be retained for legal or national security reasons.
- Records for individuals who are a match to a government watch list and are identified as a threat to transportation are kept by TSA for 99 years after issuance of a final agency

[1] TSA operates the DHS TRIP web site and the contract with Desyne is with TSA.

decision or seven years after TSA learns that the individual is deceased, whichever is shorter. After the issuance of the final agency decision, records would be transferred to NARA and may be retained for legal or national security reasons.

- After the records are no longer needed, they are destroyed according to NARA policies.

DHS Data Security Policies

1) **Please provide a copy of the Department's data security policy with respect to the collection, use, dissemination, and maintenance of personal information (e.g., Social Security Numbers, first and last names, addresses, etc.)**

   The Department's policies on the collection, use, dissemination and maintenance of personal information are outlined in Section 3.14 of *DHS Sensitive Systems Policy Directive 4300A*, **(ENCLOSURE 7)**. These policies have been widely disseminated throughout the Department and are also available on the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) intranet home pages.

2) **Does the Department utilize a process for the disposal of obsolete data in electronic form, containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable? If so, please provide a narrative describing this process. If not, why not?**

   DHS policies related to the protection and disposal of sensitive information are found in *DHS Sensitive Systems Policy Directive 4300A* **(ENCLOSURE 7)**. Section 1.4.3 of the policy directive defines "...personal data such as Social Security Number..." as being "sensitive information." The section further states: "All sensitive information must be protected from loss, misuse, modification, and unauthorized access." The following table, extracted from Section 4.3.1, explicitely governs disposal of obsolete electronic information.

Media Sanitization and Disposal

DHS Policy
a. Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.
b. Components shall maintain records of the sanitization and disposition of information systems storage media.
c. Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.

3) **For the period from May 1, 2005 to May 1, 2007, please provide the following information:**

a. **How many instances have occurred in which electronic data containing personally identifiable information maintained or collected by the Department was accessed by an unauthorized individual or individuals? For each instance, please provide the date of the breach and the actions taken by the Department to notify affected individuals and prevent a recurrence.**

b. **How many instances have occurred in which electronic data containing personally identifiable information maintained by the Department was lost or stolen? For each instance, please provide the date of the breach and the actions taken by the Department to notify affected individuals and prevent a recurrence.**

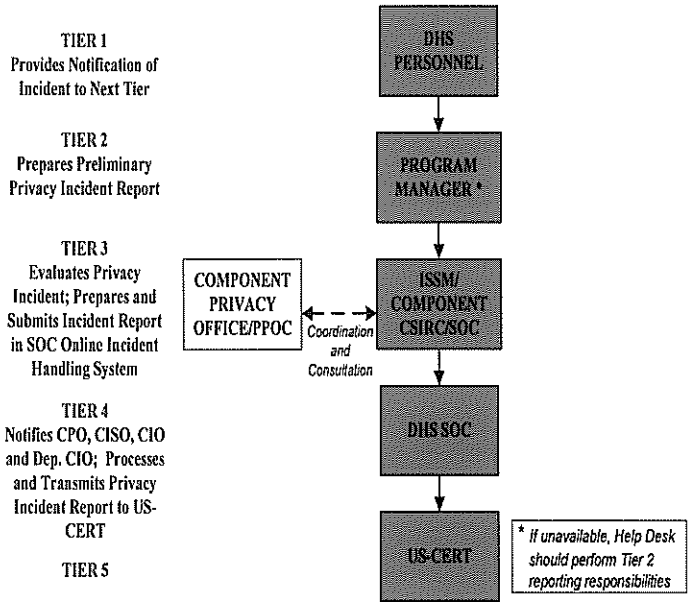
c. **In (a) and (b) above, how many of the individuals affected were Department employees?**

d. **What efforts did the Department undertake to notify the employees in question (c)? How and when were these individuals notified? If they were not notified, why not?**

Incident Reporting

During the time frame identified, the DHS Security Operations Center (SOC) reported at least 31 incidents possibly involving Personally Identifiable Information (PII) to the US-CERT. DHS maintains a summary report for all incidents reported by the DHS SOC to the US-CERT from October 2004 to the present **(ENCLOSURE 8)**.

Components are required to report incidents possibly involving PII to the DHS SOC and the DHS Privacy Office. The DHS SOC currently passes these reports on to the US-CERT, as shown in the graphic below.



Initial Incident Reporting Process for PII

Incidents reported to the DHS SOC include those where physical media (such as laptops, USB drives, hard drives, CD discs, or other media) are lost or stolen. Incidents reported also include potential intrusions, identified through a number of mechanisms such as system logs, intrusion

detection systems, system anomalies, and user notification. Intrusions that may have resulted in unauthorized access to PII are reported to the DHS SOC and the DHS Privacy Office.

Incident Response

After the initial incident report by DHS SOC to US-CERT, the DHS Privacy Office will provide updates on status and closure to US-CERT. The DHS Privacy Office coordinates remediation with the Components; the Components then notify affected individuals and take steps to prevent a recurrence of the problem.

As an example, privacy incident 2007-03-026, reported by the U.S. Coast Guard (USCG), resulted in credit monitoring services being provided to individuals. The USCG contacted the users and informed them of the incident, and users were advised to report any suspicious identity/credit activity to the Coast Guard Investigative Service (CGIS) for further action. Additionally, the National Maritime Center (NMC) is in the process of purchasing 12 months of credit monitoring for each affected applicant. Additional examples are provided in the attached table **(ENCLOSURE 8)**.

Should you require any additional information or have any additional questions, please contact Scott Charbo, Chief Information Officer, at (202) 447-3735.

Sincerely,

Paul A. Schneider
Under Secretary for Management

cc:
Scott Charbo, Chief Information Officer
Joe Peters, Transportation Security Administration Chief Information Officer

ENCLOSURES:

1. 1100 – Human Resource Listing (NARA approved file plan) **(ENCLOSURE 1)**;
2. TSA MD 200.7, *Records Management* (Assistant Administrator for Finance and Administration and Chief Financial Officer, October 9, 2002) **(ENCLOSURE 2)**;
3. TSA MD 200.8, Records Management Files Classification System (Assistant Administrator for Finance and Administration and Chief Financial Officer, January 28, 2005) **(ENCLOSURE 3)**;
4. TSA Records Management Guidance (Assistant Administrator for Finance and Administration and Chief Financial Officer, November 15, 2002) **(ENCLOSURE 4)**;
5. TSA Records Management Policy Manual (Assistant Administrator for Finance and Administration and Chief Financial Officer, December 20, 2002) **(ENCLOSURE 5)**;
6. TSA letter to impacted TSA employees and former employees **(ENCLOSURE 6)**;
7. DHS Sensitive Systems Policy Directive 4300A, V.1, dated April 18, 2007 **(ENCLOSURE 7)**; and
8. Summary report for all incidents reported by the DHS SOC to the US-CERT from October 2004 to the present (For Official Use Only) **(ENCLOSURE 8)**.